

UNITED STATES'  
EXHIBIT 4

**DECLARATION OF GARY WONG**

Pursuant to the provisions of 28 U.S.C. 1746, I hereby declare that:

1. I am the Deputy Executive Officer for the Civil Rights Division ("Division"), United States Department of Justice. I have held this position since 2012. My official duties include overseeing the Division's Information Technology ("IT") Group, which oversees the Division's computer network, including the Justice Consolidated Office Network ("JCON") system.
2. The information contained herein is based on my personal knowledge and information received in my official capacity.
3. IT maintains the Division's computer networks, the JCON computing environment, and its computer hardware, including servers, workstations, laptops and Blackberry devices. The JCON computing environment includes file and electronic mail ("email") servers, desktop operating systems, security features, productivity software such as the Microsoft Office Suite, email archiving software, and external network connectivity.
4. As of January 2014, the Civil Rights Division had 863 employees and contractors, each of whom uses a Division-owned desktop or laptop computer ("workstation") for work. Over 600 employees use Division-owned Blackberry devices to access work email and make work-related telephone calls. At present, there are a total of approximately 100 employees and contractors in the Voting Section and the Office of the Assistant Attorney General of the Civil Rights Division. I have been advised that there may be as many as 45 employees and contractors in these offices impacted by a search of records to respond to the document requests in this matter.

5. I have reviewed Defendants' First Request for Production of Documents served in *United States v. Texas*. That document requests several types of electronically stored information (ESI) that are difficult and costly to access, collect, and review. Most of the requested ESI exists to facilitate the effective functioning of the computer system and is accessible only to IT professionals.\*
6. Texas seeks a variety of temporary data, including temporary files and Internet or web-browser-generated information stored in textual, graphical, or audio format, including history files, caches, and cookies. Each of these file types is stored on the hard drive of individual workstations. Moreover, these types of data are stored in binary format, which means that they are not text-based documents that can be searched by key word.
7. Temporary files are automatically created by a computer when a user creates or edits an electronic file like a Word document, spreadsheet or presentation. The purpose of a temporary file is to insure that a user's work can be retrieved if his computer experiences a technical problem (*e.g.*, "crashes"). Computers routinely overwrite temporary files, meaning that temporary files are typically deleted when a user successfully saves a document and the application properly shuts down.
8. Internet- and web-generated information includes caches, browser history files, and cookies. Caches and browser history files are created when an individual uses a web browser like Internet Explorer or Firefox to access the Internet and intranet web applications. The computer stores information about websites visited and searches performed. A cookie is a

---

\* I am unable to determine what Texas seeks by requesting "system history files".

small piece of data used by a website to enable an individual to use the website or track the individual's activities on the website. Cookies have a fixed duration that is set by the website. The amount of Internet- and web-generated information on a single computer is voluminous. In one week, a computer may store thousands of history files, caches or cookies.

9. Texas also seeks computer activity logs that exist to record the operations of individual workstations and servers. Computer activity logs include information such as when a user logged on to a computer or when the computer contacted a server for information, started use of an application, or experienced some type of failure. These logs are voluminous, consisting of tens of thousands of entries for an individual workstation in a single week. Server activity logs record similar data for servers and constitute an enormous volume of data. In a single week, a server can generate enough data to fill over 100 DVD-ROMs.

10. Texas also seeks ESI stored on "smart cards." This category encompasses the Personal Identity Verification (PIV) cards issued to Federal employees for building access and identification and the "SmartTrip" cards used by employees who receive transit subsidies. Both PIV and SmartTrip cards contain personally identifiable and security-sensitive information of Federal employees including photos, credentials and PINs used to uniquely identify individuals. The Division does not use these "smart cards" to store any information on case-related activity.

11. Texas also seeks ESI from integrated circuit cards. This encompasses SIM cards, which are used in the Blackberry devices issued to CRT employees, and microSD cards which are used to locally store information such as photographs on Blackberry devices. SIM cards, which permit Blackberry devices to receive telephone calls, contain an individual's phone number and other information needed by telecommunications carriers to enable phone calls. Both SIM

cards and microSD cards are stored on individual Blackberry devices. The information on the cards is not available on the CRT computer network and must be collected from each individual Blackberry device.

12. Texas also seeks deleted files. The Division's computer network does not automatically delete any user-created files. Therefore, files such as Word documents, spreadsheets, and presentations continue to exist on workstations and the computer network unless: 1) a user deletes a file (either intentionally or inadvertently); or 2) there is a technical problem with the user's workstation (e.g., virus, exposure to malicious software or physical damage) which requires IT to completely replace it.

13. If a file is deleted from a workstation and that file is not also saved to the computer network, the file may be recovered from the "recycle bin" or restored by an IT professional using specialized software. Both approaches require examination of the individual workstation. Restoration of deleted files requires the use of specialized forensic software that can reconstruct parts of the file stored on the workstation's hard drive. This reconstruction involves searching the entire hard drive for fragments of the deleted file and reconnecting the available fragments. This process may or may not find entire files and will likely not restore original file names of reconstructed files and fragments.

14. In order to collect the categories of ESI described above from individual workstations and Blackberry devices, members of the IT staff would be required to:

- 1) prepare property passes enabling them to move IT equipment between buildings and travel to each building where impacted employees work (approximately 30 minutes);
- 2) copy the SIM and microSD cards of each employee's Blackberry device (approximately 15 minutes);



- 3) require the employee to log off his workstation and exchange his existing workstation for a new one (approximately 90 minutes);
- 4) secure each workstation containing the data that Texas seeks and return to the IT department (approximately 20 minutes);
- 5) make a forensic copy of the hard drive of each workstation and store that image on a secure location on the computer network (approximately four hours);
- 6) perform a forensic analysis of each hard drive copy to recover deleted items (approximately 20 hours); and
- 7) locate each category of data described above (approximately 12 hours).

15. For each impacted Division employee, I estimate that it will take approximately 38 hours to collect, locate and retrieve the requested ESI. If the IT staff were to take these steps for only the estimated 45 impacted employees and contractors in the Voting Section and the Office of the Assistant Attorney General, I estimate that it would take 1,710 hours (214 work days) to collect, locate, and retrieve the items that Texas seeks.

16. In addition to examining individual workstations and Blackberries, the IT staff would also be required to determine whether deleted files are available on the computer system's file servers. In order to continue to operate the Division's file servers during search and collection of deleted items, members of the IT staff would try to recover deleted files from the file server's backup media. The Division's backup media is designed for disaster recovery purposes, not for searching and locating individual files. If one or more servers fail, a member of the IT staff can use the backup media to restore the server, meaning that a copy of the server's data is taken from the failed server and placed on a new server. Restoring a backup system is a time-consuming process that requires:

- 1) Preparing a duplicate server environment (approximately three days); and,
- 2) Copying data from the backup media to the duplicate server (approximately five days).

17. Once a copy of the data from the file server is made, members of the IT staff would use forensic techniques similar to those used on workstations to reconstruct deleted files. I estimate that it would take approximately five days to perform a forensic analysis of data for each file server.

18. In total, I estimate that it will take 13 days to collect, locate and retrieve the items that Texas seeks from each computer server. In order to perform these tasks only for the estimated 45 impacted employees in Voting Section and the Office of the Assistant Attorney General, the IT staff would need to restore and forensically review at least two file servers, requiring approximately 26 days of work.

19. Once the information sought by Texas is gathered by the IT staff, it must be reviewed and prepared for production. The Division's Litigation Support Group would load all collected data into review software. The litigation team would review for responsiveness and privilege, while the IT staff would review for security-sensitive information. Security-sensitive information includes information that could be used by hackers or cybercriminals to undermine the IT system, including machine addresses, information about installed software, the success or failure of software updates, or the identity or structure of the internal computer environment. Security-sensitive information would need to be redacted from the responsive material. Finally, the Division's Litigation Support staff would transfer responsive, non-privileged, non-security-sensitive information to DVDs or hard drives that would be encrypted before they are sent to Texas. Given the volume of data that could be retrieved from these searches, I estimate that it would take the IT staff an additional five days to identify and redact security-sensitive information.

20. I estimate that in order to perform the search, collection, and review of ESI sought by Texas -- which requires 245 work days or 49 work weeks -- I would be required to re-assign five IT staff members from their existing duties. Those staff members are assigned to the Information Systems Branch (ISB), which has a staff of approximately 20. ISB is responsible for providing routine customer assistance and responding to emergency computer security problems (e.g., computer viruses, malware, and phishing scams) and managing and working on new and ongoing IT engineering projects. Re-assigning five ISB staff members to the search and collection of ESI sought by Texas, would effectively cut the ISB staff by twenty-five percent for the duration of this effect. Those staff members would be unable to provide any support to the Division during that project, severely hampering ISB's ability to conduct its day-to-day activities. The diversion of these staff members would substantially interfere with the IT department's work.

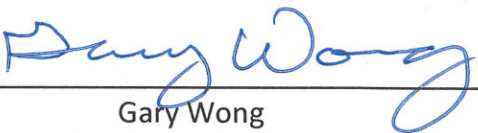
21. Finally, the Division is unable to hire contract staff to perform the search, collection and review sought by Texas. The identification, clearance, contracting, and training of contract staff can take several weeks, which would not accelerate the search and collection of ESI sought by Texas. Moreover, the forensic analysis of data from workstations and hard drives described



herein cannot be performed by contract staff because of the security-sensitive nature of some of the information sought by Texas.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 21<sup>st</sup> day of February 2014.

  
\_\_\_\_\_  
Gary Wong